

identifier, could cease unless reception of the corresponding content item was requested via another method such as from the offerings list or according to specified metadata attributes.

According to the present invention, in order for a user to access certain specific content items and/or certain types of content, subscription and/or purchase may be required. For example, a user wishing to receive all live concerts might need to subscribe to a “live concert service”. Additionally a user might be able to subscribe to a sub-service such as “all live rock concerts” or to a specific distribution such as a particular rock concert.

For example, a user selecting an item from the offerings list might be told the viewing that selection would require her to purchase a subscription. In some embodiments, the user would be given several choices for purchasing a subscription. A terminal subscriptions module running on the user's terminal may maintain in an associated store a list of all possible subscriptions that the user is eligible to purchase, noting for each one whether that subscription has been purchased. For example, upon selection of a June 22nd, 2002 live Joe Cocker rock concert from the offerings list, the terminal offerings module might query the subscriptions module to see if the user had purchased at least one subscription that would allow viewing of that concert. If the user had no eligibility to view the content, the subscriptions module could cause the following to be displayed upon the terminal screen:

“You are not currently entitled to view this program. Please indicate your selection:

- I do not wish to purchase the right to view this program
- I wish to purchase the right to view all offerings of the category ‘live musical concert’
- I wish to purchase the right to view all offerings of the category ‘like rock concert’
- I wish to purchase the right to view this program only”

If the user selected the second or third choice, she might then be asked the period of time for which she wished to subscribe.

In the case where the user selected a purchase, this request could be forwarded to the DDS subscriptions module 805, perhaps using SOAP over a GSM, satellite, landlink, or other return channel. In some embodiments the DDS subscriptions module 805 would compute the price of the purchase and forward it to the billing module 807 for verification of the user's ability to pay. The billing module might then access the user's credit card number on file and then contact a computer of the corresponding credit card company to receive authorization for a purchase of the appropriate amount. Once authorization was received, the billing module could inform the DDS subscription module of this fact. The DDS subscription module could then prepare for transmission to the user one or more access keys corresponding to the subscriptions purchased. In some embodiments, the user would not be billed until the access key or keys were distributed.

As noted above, IPSEC may be used during the multiprotocol encapsulation of content which requires subscription. The access key which will be sent to the user who purchases a particular subscription would be the key that, according to the IPSEC protocol, would allow use of the content so encapsulated. For cases where a subscription corresponds to a single event, download or the like, such as subscription to view a particular rock concert, the access key will only be useful for the viewing of that particular event and thus may not need to possess a particular expiration date since the key is inherently worthless once the event is over. On the other hand, for subscriptions which span multiple individual distributions, such as a subscription for all live musical concerts, the access key would likely be set to expire.

In some embodiments, a key for a particular service might only be valid for a day. In such a case a user might receive each day for the period of time which she chose to subscribe, a new key corresponding to the service. At the end of the chosen subscription period keys would

no longer be distributed to the user, therefore preventing her from viewing content she did not pay for.

The shorter the period of time that is selected for keys to be valid, the more choice the user has as to her subscription period. For example, if keys are selected to be valid for a day, the subscription period chosen by the user can only have a resolution of one day. Thus, a user could request a six-day subscription period but not a six-days-and-five-hours subscription period. On the other hand, if it were decided that keys would be valid for only an hour, the user could choose subscription periods with a resolution of one hour. Thus a user could choose a six-days-and-five-hours subscription period.

Furthermore, according to the present invention access keys may possess skeleton key functionality. The spirit of this functionality is shown in figure 9. In this example, access key A allows access to all live musical concerts. Access key B allows access all live rock concerts and therefore allows access to only a subset of the distributions key A allows access to. Access key C allows access to only one particular rock concert, and thus allows access to a one-member set which is a subset of both the set of distributions key A allows access to and the set of distributions key B allows access to.

Before an access key is sent to a user terminal, it is preferably encrypted such that two other keys are needed at the user terminal to perform its decryption. The first key is a terminal key 1005 which is preferably permanently built into the hardware of the terminal. The second is a user key 1001. The user key is, for example, given to the user when he initially activates his terminal. Thus it may be required that users activate their terminals at the store at which they purchase them, and that the store load the user key onto the device. In another embodiments, the user key could be distributed on removable media such as a compact flash or MMC (multimedia card) that is readable by the terminal.